■ ยืน ภู่วรวรรณ

หักเหลี่ยมทรชน บนเครือข่าย

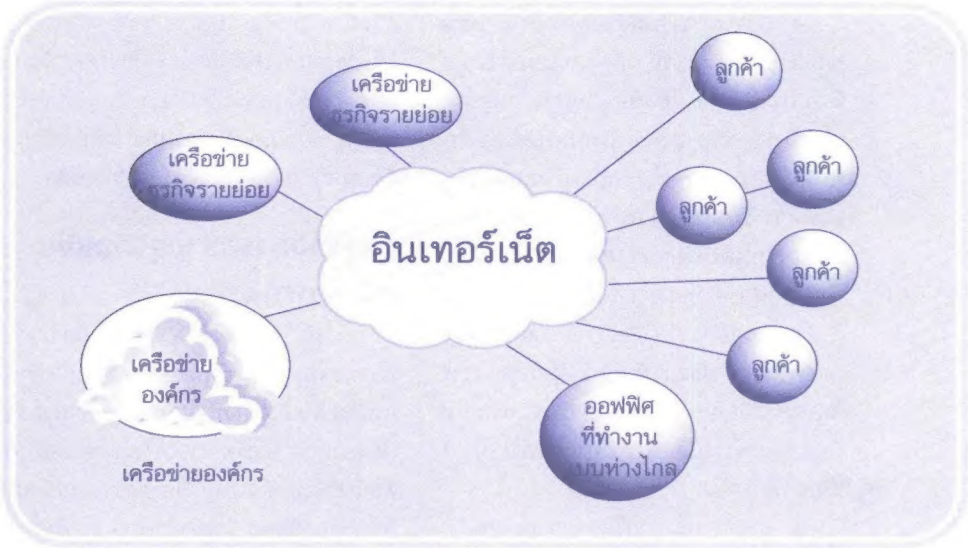
เรียนรู้พฤติกรรมการโจมตี
เพื่อสร้างระบบป้องกันการบริหาร
และระบบรักษาความปลอดภัย

เมื่อเดือนกุมภาพันธ์ ปี ค.ศ. 2000 เว็บไซท์ที่มีชื่อหลายแห่ง เช่น yahoo, amazon, ebay ได้รับการโจมตีจากภายนอก ลักษณะการโจมตีเกิดจากการเรียกจากภายนอกจำนวนมาก เข้ามาพร้อมกัน ทำให้ระบบเซิร์ฟเวอร์ไม่สามารถสร้างการเชื่อมโยงเพื่อการให้บริการพร้อมกันได้ ทำให้เว็บเซิร์ฟเวอร์เหล่านั้นหยุดการให้บริการลง หรือบริการได้ช้าลง

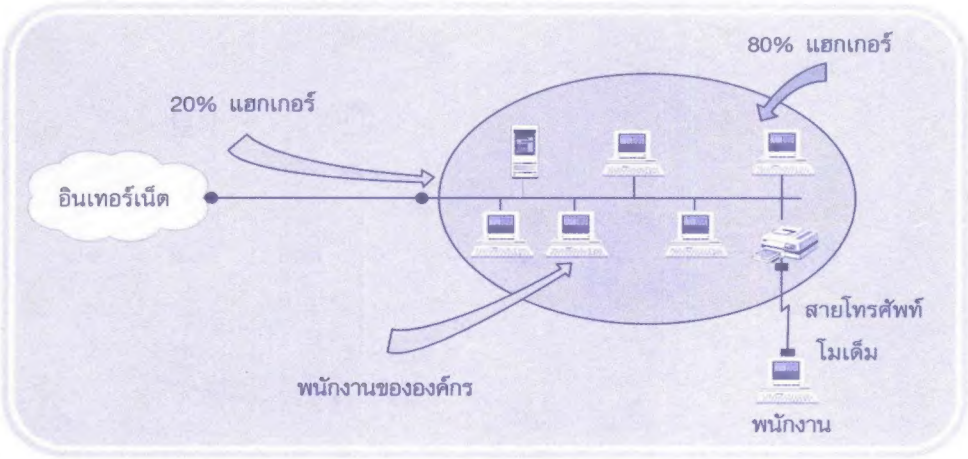
ในประเทศไทยก็มีปัญหาในเรื่องที่แฮกเกอร์บุกเข้าเซิร์ฟเวอร์ของไอเอสพี และนำข้อมูลลูกค้าที่ใช้บัตรเครดิต นอกจากนี้ก็มีการแอบเข้าวางกับดักเพื่อลักลอบลักข้อมูลรหัสผ่านเข้าใช้อินเทอร์เน็ตหรือนำรหัสผ่านออกไปใช้งานในทางที่ไม่ถูกต้อง

ลักษณะของการบุกรุกเข้าสู่เครือข่าย

เครือข่ายอินเทอร์เน็ตเป็นเครือข่ายสาธารณะที่มีผู้ใช้ภายนอกจำนวนมากอีกทั้งการดำเนินงานเฉพาะภายในองค์กร ก็จำเป็นที่จะต้องให้ข้อมูลผ่านอินเทอร์เน็ต เช่นการดำเนินงานแบบอีคอมเมิร์ซ อีบิสิเนส การแลกเปลี่ยนข้อมูล (EDT) ระหว่างหน่วยงานทั้งหน่วยงานภายในของตนเอง และหน่วยงานภายนอก การเคลื่อนย้ายข้อมูลผ่านเครือข่ายสาธารณะย่อมไม่ปลอดภัย และอาจมีผู้ทำการคัดลอกข้อมูลออกไปได้ การดำเนินการทางธุรกิจบนเครือข่ายอินเทอร์เน็ตจึงอยู่บนพื้นฐานของความเสี่ยงตลอดเวลา



รูปที่ 1 โมเดลที่อินเทอร์เน็ตเป็นเส้นทางข้อมูลเชื่อมโยงการทำงานแบบต่าง ๆ



รูปที่ 2 ปัญหาใหญ่อยู่ที่บุคคลภายในองค์กร

ข้อมูลแบบแพ็กเก็ตที่วิ่งอยู่บนอินเทอร์เน็ตมีข้อมูลที่บอกต้นทางและปลายทางจึงเป็นข้อมูลที่สามารถแยกแยะและคัดลอกหรือเปลี่ยนแปลงข้อมูลได้ การดำเนินการในเรื่องการบุกรุก หรือโจรกรรมข้อมูลจึงเกิดขึ้นได้ทุกหนทุกแห่งบนเครือข่ายคอมพิวเตอร์ จากข้อมูลของหน่วยวิจัยทางด้านการรักษาความปลอดภัยของระบบพบว่าการบุกรุกและการดำเนินการในเรื่องการเจาะระบบ การฝ่าเข้าสู่ระบบรักษาความปลอดภัย หรือการทำโจรกรรมข้อมูลข่าวสารต่าง ๆ เกิดจากบุคคลภายนอกองค์กร ที่มาจากอินเทอร์เน็ตประมาณ 20 เปอร์เซ็นต์ แต่เกิดจากบุคคลหรือพนักงานภายในองค์กรเองถึงประมาณ 80 เปอร์เซ็นต์ นั่นหมายความว่า บุคคลภายในที่ผ่านเข้าออกระบบได้จะเป็นผู้ที่สร้างปัญหาให้องค์กรมากกว่า

ดังนั้นระบบรักษาความปลอดภัยจึงมิได้กระทำขึ้นเพื่อป้องกันบุคคลภายนอกเท่านั้น เครือข่ายภายในและบุคคลภายในองค์กรก็เป็นปัญหาใหญ่ อีกทั้งระบบภายในที่เปิดให้ผู้ใช้ภายในเข้าถึงระดับหนึ่งจึงง่ายที่จะลักลอบผ่านด่านปลอดภัยต่าง ๆ แม้บางเครือข่ายที่ไม่ได้ต่อกับอินเทอร์เน็ตก็มีโอกาสได้รับการบุกรุกได้เช่นกัน

ข้อมูลการสำรวจทั่วไป จากบริษัทซิสโกกล่าวไว้ว่า การบุกรุกและโจมตี หรือเข้ามาในเครือข่ายและโฮส กว่าร้อยละ 75 ไม่สามารถตรวจจับและรับรู้ได้ มีเพียงประมาณ 20 เปอร์เซนต์เท่านั้นที่ตรวจสอบหรือรับรู้ และประมาณ 80-85 เปอร์เซนต์ที่เป็นบุคคลภายในจะเป็นบุคคลที่องค์กรให้ความเชื่อถือ

ปัญหาที่ประสบมากขณะนี้อีกอย่างหนึ่งคือปัญหาจากแฮกเกอร์สมัครเล่น ที่นำเครื่องมือ โปรแกรม หรือวิธีการต่าง ๆ จากอินเทอร์เน็ตจากเพื่อนฝูง นำมาทดลองเจาะระบบ หรือ เข้าทางจุดอ่อนของระบบโปรแกรมเจาะระบบต่าง ๆ มีมากมาย รวมทั้งมีเว็บไซท์หลายแห่งให้วิธีการและขั้นตอนการเจาะระบบอย่างชัดเจน รวมทั้งการแจกจ่ายเครื่องมือหรือโปรแกรมบางอย่างให้นำไปใช้ทดลอง สำหรับแฮกเกอร์มืออาชีพ หรือแฮกเกอร์ที่มีประสบการณ์แล้ว การตรวจจับหรือการดำเนินการให้ถึงจุดต้นทาง เป็นสิ่งที่กระทำได้ยาก เพราะแฮกเกอร์พวกนี้จะระมัดระวังและหาทางที่จะปกปิด เช่นใช้จุดดำเนินการตามสถานที่ที่ยากต่อการตรวจสอบ เช่น อินเทอร์เน็ตสาธารณะต่าง ๆ

ทำไมต้องสนใจในเรื่องระบบการรักษาความปลอดภัย

ในช่วงสิบปีที่ผ่านมาขีดความสามารถของคอมพิวเตอร์สูงขึ้นมาก ระดับการเรียนรู้ทางเทคโนโลยีของประชาชนทั่วไปก็สูงขึ้น จำนวนประชากรที่เรียนรู้คอมพิวเตอร์มีมาก และสามารถหาแหล่งความรู้ต่าง ๆ ได้ง่าย ระดับความรู้ของผู้ที่ใช้ในทางที่ไม่ถูกต้องก็มีมากขึ้น ประจวบกับการเจริญก้าวหน้าของเครือข่ายทำให้การเข้าถึงทรัพยากรและแหล่งข้อมูลได้ง่ายขึ้น ด้วยเหตุผลดังกล่าวทำให้แนวโน้มของปัญหาการรักษาความปลอดภัยมีแนวโน้มที่ซับซ้อนและยุ่งยากมากขึ้น จากสถิติของผู้บุกรุกบนเครือข่ายเพิ่มขึ้นเป็นสองเท่า ทุก ๆ ประมาณ 3 ถึง 4 ปี ทำให้ตัวเลขความเสียหายและการลงทุนที่ต้องเพิ่มขึ้นทุกปี

การดำเนินการในเรื่องรักษาความปลอดภัย

การบุกรุกเข้ามายังเครือข่ายของแฮกเกอร์โดยมีเป้าหมายคือลักลอบเข้ายังเครื่องบริการต่าง ๆ ด้วยการบุกรุกผ่านด่านป้องกันต่าง ๆ โดยปกติแฮกเกอร์จะโจมตีจุดที่เปราะบางและอ่อนแอที่สุดของระบบก่อน เมื่อเข้าได้แล้วจะใช้เป็นฐานในการปฏิบัติต่อส่วนต่าง ๆ ต่อไป จากประสบการณ์ของผู้ดูแลระบบทั่วไปพบว่าการบุกรุกเข้าสู่เครือข่ายจากภายนอกมักจะมาจากฐานที่ถูกโจมตีและเข้าควบคุมการทำงานก่อน การใช้ฐานจากที่ต่าง ๆ ทำให้ติดตามได้ยากและพรางการกระทำได้ง่าย

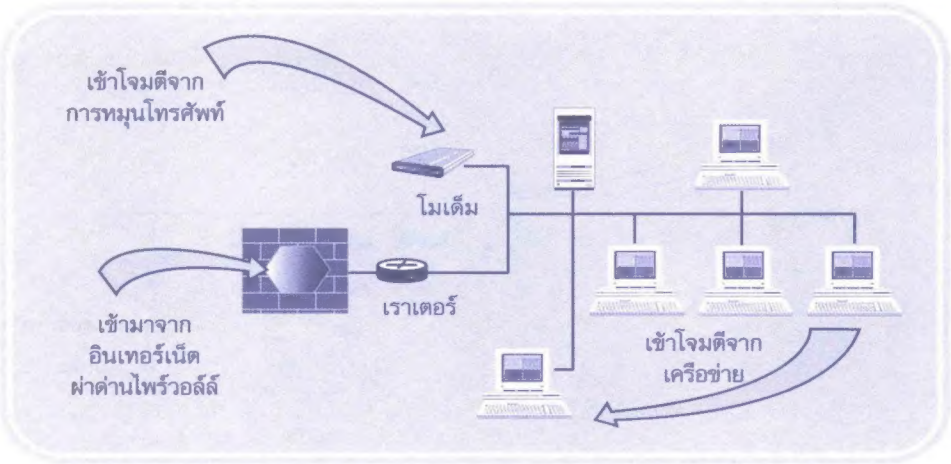
การดำเนินการในเรื่องระบบรักษาความปลอดภัยต้องกระทำเป็นระบบ ทั้งนี้เพราะการเปิดจุดรั่วไหล หรือจุดอ่อนของระบบ ย่อมทำให้เป็นช่องทางการเข้าสู่เครือข่ายและโจมตีเข้าสู่ระบบ เป็นฐานให้เข้าถึงจุดอื่น ๆ ได้ง่าย

สิ่งที่จะต้องดำเนินการในระบบรักษาความปลอดภัยประกอบด้วย

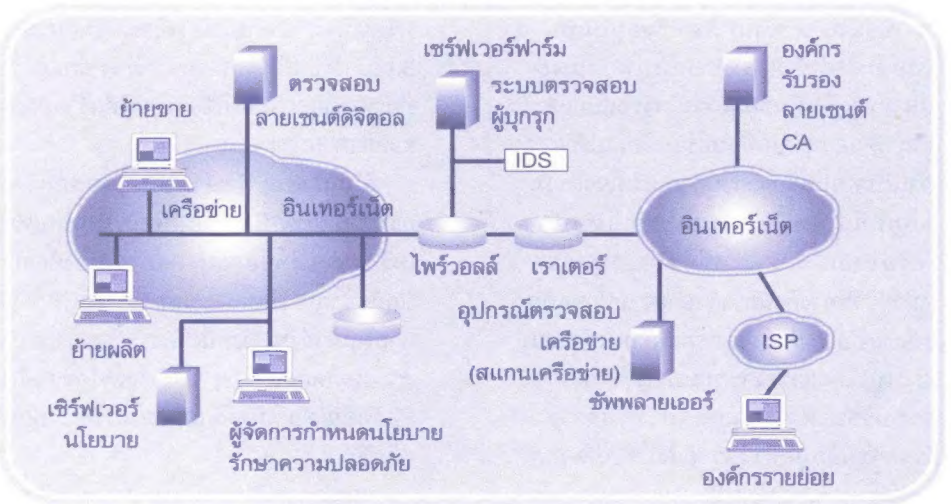
- การกำหนดและตรวจสอบตัวบุคคลผู้ใช้ (identity) เป็นการกำหนดรหัสผู้ใช้โดยเน้นให้ผู้ใช้ภายในองค์กรใช้รหัสผ่าน (password) โดยเน้นการดูแลรหัสผ่านของตนเองเป็นพิเศษโดยต้องไม่ให้รหัสผ่านของตนเองรั่วไหลไปยังผู้อื่น ต้องไม่ตั้งรหัสผ่านที่ง่ายเกินไป ต้องปฏิบัติตามกฎเกณฑ์ขององค์กรอย่างเคร่งครัด
- การควบคุมการเข้าออก (perimeter security) เป็นการสร้างจุดควบคุมการเข้าออกเช่นการวางเกตเวย์ การใช้ไฟร์วอลล์ การเข้าออกระบบทุกระบบจะมีการตรวจสอบและบันทึกการเข้าใช้งาน การตรวจสอบการเข้าใช้ทรัพยากร และตรวจสอบการทำงาน การบันทึกข้อมูลต่าง ๆ เกี่ยวกับการเข้าใช้ งาน รวมถึงการวิเคราะห์และป้องกันการบุกโจมตีเครือข่าย
- การจัดการรับส่งข้อมูลเฉพาะ (data privacy) เป็นการกำหนดส่วนของข้อมูลที่เป็นเฉพาะตัว เช่นข้อมูลจดหมายอิเล็กทรอนิกส์ ข้อมูลที่ใช้เฉพาะบุคคลหรือเฉพาะกลุ่ม (workgroup) การติดต่อกับองค์กรหรือหน่วยงานอื่นก็มีการวางท่ออุโมงค์ข้อมูลที่เรียกว่า VPN เพื่อแยกแยะการเป็นส่วนตัวของการเชื่อมโยง
- การเฝ้าระวัง (Security monitoring) การตรวจสอบและเฝ้าระวังผู้บุกรุก การวิเคราะห์ปัญหา ตลอดจนการสร้างระบบป้องกันอัตโนมัติเพื่อเตือนหรือบ่งบอกปัญหาที่เกิดขึ้น
- การวางนโยบายรักษาความปลอดภัย เป็นการสร้างกฎเกณฑ์และการควบคุมการทำงานของระบบ การวางรูปแบบการบริหารงาน การจัดโครงสร้างระบบฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่าย การกำหนดสิทธิหน้าที่ ของบุคคลในองค์กร ตลอดจนการกำหนดวิธีการติดตั้งระบบอุปกรณ์ต่าง ๆ

ตัวอย่างการสร้างธุรกิจแบบ eCommerce

สมมุติว่าบริษัท XYZ ต้องการเปิดกิจการแบบ eCommere มีการนำสินค้านำเสนอขายต่อลูกค้าทั่วไป และลูกค้าประจำที่เป็นองค์กร บริษัท XYZ ยังต้องผลิตสินค้า ดังนั้นจึงใช้เครือข่ายเพื่อดำเนินการภายในอีกทั้งต้องติดต่อกับผู้ขายวัตถุดิบนำสินค้ามาเข้าร้านจากบริษัท หรือองค์กรอื่นที่เชื่อมโยง



รูปที่ 3 เส้นทางการเข้าโจมตีระบบ



รูปที่ 4 โมเดลการทำธุรกิจแบบ eCommerce และ eBusiness

กันด้วยเครือข่าย การติดต่อสื่อสารจึงมีทั้งแบบอินทราเน็ตและเชื่อมโยงกับลูกค้า และซัพพลายเออร์ผ่านทางอินเทอร์เน็ต โมเดลของบริษัท XYZ เป็นดังรูปที่ 4

โมเดลของระบบดังกล่าวจึงประกอบด้วยกลไกการทำงานที่สำคัญ ดังนี้

- การกำหนดและตรวจสอบตัวบุคคลผู้ใช้ (identity) ปัจจุบันมีระบบลายเซนต์ดิจิตอล (digital signature) เช่น เมื่อต้องการติดต่อกับซัพพลายเออร์ในการสั่งสินค้า การส่งใบสั่งซื้อสินค้าจำเป็นต้องมีการกำหนดลายเซนต์ดิจิตอล ดังนั้นจึงต้องมีวิธีการกำหนดให้รู้ว่าใบสั่งซื้อเป็นใบสั่งซื้อที่ถูกต้อง ระบบลายเซนต์มีการกำหนดและมีการรับรองโดย CA

- การควบคุมการเข้าออก (Perimeter Security) ระบบที่ใช้ในกรควบคุมการเข้าออกได้แก่ ไฟร์วอล (five wall) ลูกค้าที่เป็นลูกค้ารายย่อยจะใช้งานผ่านไอเอสพี เมื่อจะเข้าออกจะมีการตรวจสอบและเก็บบันทึกเพื่อตรวจดูว่าเข้ามาจากที่ใด มีจุดประสงค์เพื่ออะไร ระบบการตรวจสอบการเข้าออกจึงเป็นหนทางที่จะควบคุมข้อมูลทุกแพ็กเก็ตที่จะผ่านเข้าออก โดยจุดเชื่อมต่ออินเทอร์เน็ตควรเป็นจุดที่สามารถตรวจสอบและบันทึกข้อมูลการเข้าออกได้

- การจัดการรับส่งข้อมูลเฉพาะ (Data Privacy) การติดต่อสื่อสารระหว่างกันผ่านทางเครือข่ายอินเทอร์เน็ตซึ่งเป็นเครือข่ายสาธารณะย่อมมีปัญหาและอาจมีผู้แอบดักข้อมูลได้ ดังนั้นระบบการติดต่อสื่อสารผ่านทางอินเทอร์ระหว่างผู้รับกับผู้ส่ง เช่น ลูกค้าจะซื้อสินค้าต่องส่งหมายเลขรหัสบัตรเครดิตและลายเซนต์บางอย่างจำเป็นต้องมีการเปิดช่องพิเศษที่เรียกว่า SSL-Secure Socket Layer หรือลูกค้าต้องการติดต่อสื่อสารกับบริษัทโดยเปิดช่องพิเศษที่เรียกว่า VPN การกำหนดช่องสื่อสารพิเศษเพื่อความมั่นใจว่าข้อมูลที่ส่งรับจะเป็นข้อมูลที่เฉพาะกับผู้รับและผู้ส่งเท่านั้น

- การเฝ้าระวัง (Security Monitoring) ในกิจการธุรกิจของบริษัท XYZ ตามที่ยกตัวอย่าง มีการติดตั้งระบบ IDS-Intrusion Detection System หรือระบบตรวจจับการบุกรุก ระบบดังกล่าวจะทำการตรวจสอบข้อมูลเข้าออกและข้อมูลที่เชื่อมโยงในเครือข่าย เพื่อนำข้อมูลเหล่านั้นมาวิเคราะห์ดูว่ามีส่วนใดทำการรับ หรือมีต้นใดเป็นข้อมูลบุกรุกเข้ามาจากแฮกเกอร์ ระบบ IDS ได้รับการพัฒนามาเพื่อดำเนินการตามหน้าที่ที่กำหนดไว้ในนโยบายและวิเคราะห์ความผิดปกติ หรือความโน้มเอียงที่อาจจะผิดปกติได้ เช่น การเข้าออกของข้อมูลเกินความเป็นจริง การเข้าออกของข้อมูลที่มาจากแหล่งหรือปลายทางที่ไม่ได้กำหนดไว้ ระบบ IDS จะติดต่อกับอุปกรณ์ในเครือข่ายต่าง ๆ เช่น จากเราเตอร์ จากสวิตช์ หรือจากโฮสเซิร์ฟเวอร์หลักเพื่อนำข้อมูลไปวิเคราะห์

- การวางนโยบายรักษาความปลอดภัย ปัจจุบันมีซอฟต์แวร์ที่ใช้ในการควบคุมซอฟต์แวร์ดังกล่าวรับข้อมูล นโยบายและกฎเกณฑ์ต่าง ๆ ที่องค์กรต้องการ แล้วนำนโยบายเหล่านั้นมาแปลเข้าสู่ทางปฏิบัติ โดยจะส่งข้อมูลให้กับระบบ IDS เพื่อใช้ในการตรวจสอบระบบ ส่งให้กับเราเตอร์เพื่อควบคุมพื้นฐาน ส่งให้กับเซิร์ฟเวอร์เพื่อสร้างเงื่อนไขการเข้าออกต่าง ๆ เป็นต้น

การทำงานขององค์กรเช่น บริษัท XYZ ที่ยกตัวอย่างมานี้จำเป็นที่จะต้องรวบรวมฟังก์ชันการทำงานต่าง ๆ เข้าด้วยกัน โดยเริ่มจากการกำหนดนโยบายแล้วแปลผลไปยังอุปกรณ์ต่าง ๆ ได้อย่างอัตโนมัติ

- การประยุกต์มีลักษณะซับซ้อนขึ้น การประกอบการทางธุรกิจในปัจจุบันมีความซับซ้อนขึ้น เครือข่ายเป็นเครื่องมือที่ช่วยการเชื่อมโยง อย่างไรก็ตามการดำเนินการทางธุรกิจย่อมมีคุณค่าที่เกี่ยวพันกับธุรกิจ ดังนั้นระบบการรักษาความปลอดภัยจึงต้องพิจารณาตามเงื่อนไขของคุณค่าที่เกิดขึ้นในระบบธุรกิจ เช่นถ้าระบบธุรกิจเป็นเพียงการเผยแพร่ข้อมูลสู่สาธารณะผ่านทางอินเทอร์เน็ต การเชื่อมโยงก็เสมือนการสร้างเว็บเซิร์ฟเวอร์สำหรับบริการบนเครือข่ายอินเทอร์เน็ต และหากยังไม่มีการดำเนินธุรกิจบนเครือข่าย หรือเกี่ยวข้องกับเซิร์ฟเวอร์ที่จะรับรายการคำสั่งซื้อ ระบบรักษาความปลอดภัยก็ยังไม่ต้องลงมากนัก แต่หากเป็นการดำเนินแบบ eBusiness ที่มีการรับส่งคำสั่งรายการย่อยระหว่างกัน แต่ละรายการย่อยมีความสำคัญ ในกรณีนี้ก็ต้องมีการพิจารณาระบบรักษาความปลอดภัย เช่น การใช้ VPN หรือการใช้เอ็กซ์พาเร็ต

- การบุกรุกและการโจมตีมีเทคนิคที่แยบยล เป็นที่ยอมรับว่าจุดอ่อนในระบบตั้งแต่ตัวฮาร์ดแวร์ โอเอส โปรแกรมระบบตลอดจนโปรแกรมประยุกต์ต่าง ๆ มีมาก และมีผู้ค้นพบจุดอ่อน หรือช่องโหว่ของการเจาะเข้าทำลายได้อยู่ตลอดเวลา ยิ่งระบบสื่อสารที่รวดเร็ว การแพร่กระจายข่าวสารบางอย่างในกลุ่ม แฮกเกอร์บนอินเทอร์เน็ตทำได้ง่ายและรวดเร็ว

- การเข้าโจมตีด้วยบัฟเฟอร์โอเวอร์โฟลว์ เป็นการยึด การควบคุมระบบ (root admin) ที่รู้จักกันดี โดยใช้โปรแกรมที่เขียนขึ้นเพื่อส่งข้อมูลเข้าไปยังเซิร์ฟเวอร์ ให้เซิร์ฟเวอร์มีอาการทำงานช้าลง จนถึงขั้นเกิดโอเวอร์โฟลว์ที่บัฟเฟอร์ เมื่อเกิดภาวะดังกล่าว โปรแกรมอาจหยุดปฏิบัติงานและเกิดการทำงานผิดพลาด จังหวะที่ทำงานผิดพลาดนี้ โปรแกรมของผู้บุกรุกก็จะสื่อการโต้ตอบ หรือรับการตอบสนองเสมือนเป็นผู้ดูแลระบบ

ในระบบปฏิบัติการทั้งยูนิกซ์ และเอ็นที มีจุดอ่อนที่ได้รับการค้นพบและใช้ได้ผลมาแล้ว ฝ่ายผู้พัฒนาซอฟต์แวร์โอเอสก็จะหาทางปรับปรุงแก้ไขจุดอ่อนต่าง ๆ เหล่านี้ และสร้างเป็นโปรแกรมแก้ไขระบบ ซึ่งผู้ใช้โอเอสเดิมส่วนใหญ่ไม่ได้ติดตามแก้ไขตาม ทำให้จุดอ่อนเหล่านี้ยังอยู่ในเครื่องที่ติดตั้งบนอินเทอร์เน็ตอีกมากมาย

- เน็ตสแกน เป็นวิธีการในการสแกนหาเครื่องที่ต่ออยู่บนเครือข่าย เพื่อเป็นเป้าหมายการเข้าโจมตี การหาเครื่อง (host) ทำได้ง่ายด้วยการส่งคำสั่ง ping เพื่อรองรับคำตอบกลับ มีการสร้างโปรแกรมสแกนเครื่องที่เรียกว่า ping sweep และยังสแกนพอร์ต เพื่อดูว่าเครื่องดังกล่าวเปิดช่องทางติดต่อเข้าเครื่องทางพอร์ตใดได้บ้าง เน็ตไซบาร์ยังมีวิธีการดูข้อมูลจากดีเอนเอสเพื่อหาชื่อเครื่องที่จดทะเบียนไว้ มีระบบการเก็บข้อมูลที่รับส่งเพื่อวิเคราะห์หาเป้าหมายที่จะบุกรุกต่อในส่วนปลายทาง การสแกนยังมี

ขีดความสามารถที่จะตรวจสอบว่าเครื่องใดที่กำลังทำงาน และอุปกรณ์ที่ต่ออยู่กำลังทำงานอะไร เป็นอุปกรณ์ชนิดใด

- สนิฟเฟอร์ (sniffer) เป็นโปรแกรมเล็ก ๆ ที่แฮกเกอร์แอบนำมาติดตั้งไว้ในเครื่องใดเครื่องหนึ่ง เพื่อทำหน้าที่คัดลอกข้อมูลบนเครือข่ายในระดับแน็กเก็ตเพื่อนำข้อมูลเหล่านั้นไปวิเคราะห์ และหาทางนำกลับมาใช้ในการเจาะเข้าสู่ระบบอื่นต่อไป ปกติข้อมูลบนเครือข่ายที่อยู่ในเซกเมนต์เดียวกันที่มีการเชื่อมต่อแบบบิสจะกระจายข้อมูลถึงกันทุกเครื่อง ดังนั้นระบบปัจจุบันจึงหันมาใช้สวิตช์เพื่อไม่ให้กระจายข้อมูลออกไปบนเครือข่ายให้กว้างนัก เพราะจะเป็นปัญหาต่อไปได้
- การปลอมแหล่งต้นทาง เรียกว่า Spoofing แฮกเกอร์รู้ว่าบางเครือข่ายหรือบางโฮสมีการตรวจสอบแหล่งต้นทางว่ามาจากไอพีใด ดังนั้นจึงต้องปลอมแอดเดรสต้นทาง เพื่อหลอกให้เห็นว่า เป็นเครื่องมาจากต้นทางที่จะปล่อยให้เข้าระบบได้
- การโจมตีแบบ Smrut เป็นวิธีการส่งคำสั่ง ICMP หลอกเข้ามาในเครือข่ายเพื่อให้เครือข่ายกระจายข้อมูล (Boardcast) ทำให้ข้อมูลที่กระจายตัวบนเครือข่ายมีจำนวนมาก สร้างปัญหาให้กับระบบเครือข่าย
- การฝังรหัสแบบส่งไวรัส ไวรัสคอมพิวเตอร์เป็นปัญหาใหญ่ปัญหาหนึ่งที่แพร่กระจายบนเครือข่ายได้ง่าย โดยเฉพาะการส่งผ่านทางเมล์ซึ่งผู้รับไม่ทราบก็จะคลิกเปิดดู โปรแกรมไวรัสจะฝังตัวเองไปในระบบซึ่งจะทำงานตลอดไปได้ ไวรัสบางตัวได้รับการโปรแกรมให้เก็บข้อมูลส่งต่อ หรือเก็บข้อมูลบางอย่างที่สำคัญส่งออกไปยังจุดหมายปลายทางที่ต้องการ เช่นการเก็บรหัสผ่านของโปรแกรมประยุกต์บางโปรแกรม เก็บข้อมูลที่ผู้ใช้สั่งทางแป้นพิมพ์ ไวรัสหลายตัวส่งกระจายการทำงานได้เอง เช่น ส่งอีเมล์ไปยังผู้อื่นตามรายชื่อที่ฝากๆ อยู่ในระบบอยู่แล้ว ทำให้โอกาสของการกระจายไวรัสได้เร็วยิ่งขึ้น การกระจายตัวจึงใช้เวลาเพียงสองสามวันก็กระจายได้ทั่วโลก และแพร่หลายไปทั่วเหมือนที่เคยตกเป็นข่าวมาแล้ว

บอมบ์ และ DOS - Denial of Service

การบอมบ์เป็นการส่งข้อมูลจากที่หนึ่งหรือหลาย ๆ ที่ไปยังเป้าหมายที่เดียวหรือเครือข่ายหนึ่ง เพื่อให้มีปริมาณข้อมูลเข้าถึงมากมายจนเซิร์ฟเวอร์หรือเครือข่ายเป้าหมายรับไม่ไหวและอาจหยุดการทำงานลง

วิธีบอมบ์ที่ง่ายและเกิดขึ้นเสมอคือการส่งอีเมล์จำนวนมากไปที่เซิร์ฟเวอร์เป้าหมาย โดยอีเมล์ที่ส่งไปอาจมีข้อมูลขนาดใหญ่ เพื่อให้เกิดการล้นบัฟเฟอร์ เป็นผลทำให้เซิร์ฟเวอร์ปฏิเสธการรับอีเมล์ฉบับอื่นทั้งหมด

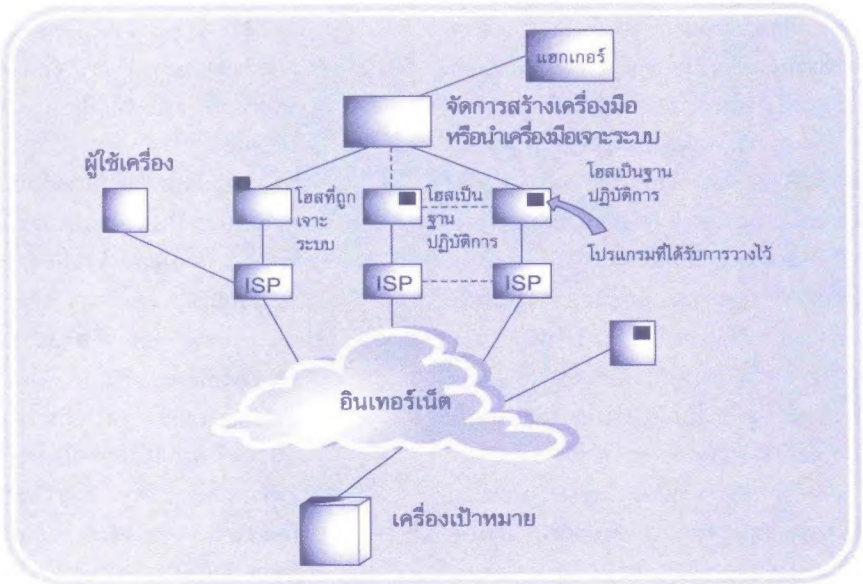
การโจมตีที่มีลักษณะซับซ้อนและแยบยลขึ้น คือ DOS การดำเนินการจะทำให้ยากต่อการตรวจสอบ วิธีการของผู้ปฏิบัติคือการเจาะระบบเซิร์ฟเวอร์บนอินเทอร์เน็ตจำนวนมากโดยไม่ให้เจ้าของรู้ตัว วางโปรแกรมไว้ในเครื่องที่เจาะระบบแล้ว โปรแกรมเหล่านั้นจะเก็บตัวเงียบรอเวลา ครั้นเมื่อถึงเวลาก็จะปลุกตัวเองขึ้นมาปฏิบัติงาน ส่งคำสั่งขอใช้บริการไปยังเป้าหมาย ผลคือ มีคำขอใช้บริการจากที่ต่าง ๆ พร้อมกันเป็นจำนวนมาก

หลังจากเดือนกุมภาพันธ์ที่เกิดเหตุการณ์ DOF ครั้งใหญ่ หน่วยงาน IETF Internet Engineering Task Force ได้ตั้งกลุ่มคณะทำงานเพื่อศึกษาและให้ข้อมูลระหว่างกัน โดยเฉพาะผู้ผลิตอุปกรณ์สื่อสารเราเตอร์เพื่อเน้นการพัฒนาระบบโอเอส ขึ้นมาให้ข้อมูลระหว่างกัน ระบบจะวิเคราะห์หาเส้นทางและจุดร่วมบางอย่างเพื่อใช้เป็นข้อมูลตรวจสอบ DOS นอกจากนี้ยังมีการทำงานร่วมกับ ISP เพื่อติดตามการโจมตีและดูเส้นทางข้อมูลที่ผิดปกติ

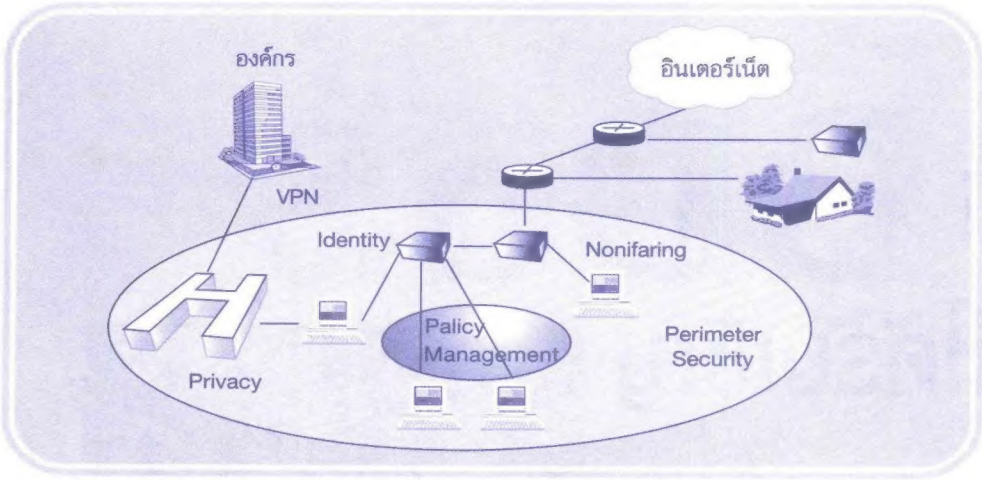
การสร้างระบบป้องกัน

ระบบป้องกันเป็นสิ่งที่ผู้พัฒนาระบบฮาร์ดแวร์ ซอฟต์แวร์ และโปรแกรมประยุกต์ได้พยายามพัฒนา ระบบป้องกันที่ออกแบบและสร้างขึ้นเป็นสิ่งที่แทรกเข้าอยู่ในระบบซึ่งก็ทำให้ประสิทธิภาพโดยรวมของระบบตกไป เช่นระบบไฟล์วอล ระบบฟิลเตอร์ ระบบ IDS-Intrusion Detection System ในอุปกรณ์สื่อสารจำพวกเราเตอร์มีการวางระบบโอเอสที่ได้พัฒนาเพิ่มเติมอยู่ตลอดเวลา ให้โอเอสทำหน้าที่กลั่นกรอง เช่นการยอมให้แพ็กเก็ต PCMP แบบใดผ่าน แบบใดไม่ให้ผ่าน การฟิลเตอร์แน็กเก็ตที่ปลอมแอดเดรสให้เป็นแอดเดรสภายในและวิ่งเข้ามาในเครือข่าย การฟิลเตอร์บางรูปแบบการใช้งานรวมถึงการสร้าง VPN เพื่อใช้ในงานสื่อสารระหว่างกัน

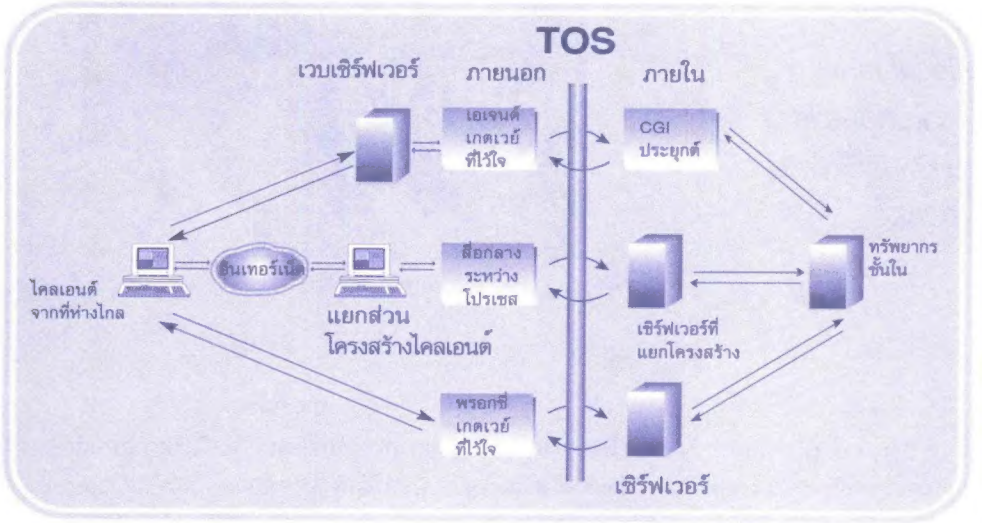
ระบบป้องกันจึงมีความสลับซับซ้อนขึ้น ดังนั้นจึงต้องทำให้ง่ายต่อการดูแล และใช้งานโดยรวมฟังก์ชันต่าง ๆ เข้าด้วยกัน เพื่อให้บริการและจัดการระบบได้ที่ส่วนกลาง



รูปที่ 5 การใช้โฮสบนเครือข่ายจำนวนมากเป็นฐานปฏิบัติการ DOSกับโฮสเป้าหมาย



รูปที่ 6 การบริหารระบบรักษาความปลอดภัยให้เป็นหนึ่งเดียว



รูปที่ 7 รูปแบบ TOS ที่แยกการทำงานเป็นโปรเซสย่อยและให้แต่ละโปรเซสมีสถานะระดับต่ำที่ไม่มีสิทธิพิเศษใด ๆ

การจัดการระบบรักษาความปลอดภัยเกี่ยวข้องกับเรื่องของการกำหนดบุคคล การสร้างช่องสื่อสารเฉพาะ การวางโครงสร้างการตรวจสอบระบบ และเชื่อมโยงผู้ใช้รวมถึงนโยบายที่สำคัญของการรักษาความปลอดภัย ระบบดังกล่าวจึงต้องเชื่อมโยงและบริหารจัดการจากที่เดียวเพื่อควบคุมกลไกการทำงานทั้งองค์กร

แนวทางใหม่ในการสร้างโอเอสที่ไว้ใจได้ Trusted OS

จุดอ่อนของระบบในปัจจุบันอย่างหนึ่งคือระบบโอเอส ระบบโอเอสที่พัฒนาขึ้นมามีลักษณะที่ผู้อยู่ภายนอกจะเข้าถึงตัวโปรแกรมโอเอสได้ง่าย ดังนั้นจึงหาทางให้โปรแกรมเบรกตัวเองขณะทำงานแล้วเชื่อมต่อโปรแกรมที่จัดสร้างขึ้นเพื่อเข้าไปควบคุมระบบได้

ในโปรแกรมประยุกต์ที่ใช้งานกันอยู่ในขณะนี้ต้องผ่านโอเอส เพื่อเข้าไปจัดการกับระบบการจัดการระบบของโอเอสมีสิทธิเท่ากับ root หรือสิทธิสูงสุด เพื่อเขียนอ่านไฟล์ ดังนั้นระบบโปรแกรมประยุกต์ที่ใช้งานจึงเป็นเส้นทางที่จะเชื่อมกับโอเอสและทำให้แฮกเกอร์ใช้ประโยชน์ส่วนนี้ได้

ทางแก้ไขทางหนึ่งคือการออกแบบระบบโอเอสใหม่ โดยแบ่งแยกโอเอสออกเป็นส่วนให้ชัดเจน เพื่อแยกผู้ใช้ที่อยู่ภายนอกไม่ให้เข้าถึงระดับ root ได้ โดยแยกกลไกการทำงานระดับโปรแกรมประยุกต์ ให้เข้าถึงข้อมูลที่ระดับสิทธิเฉพาะต่ำ คือไม่สามารถทำงานได้ทุกอย่างเช่น root

การแยกส่วนของโอเอส และสร้างระบบเชื่อมต่อใหม่ ทำให้หนทางที่บุคคลภายนอกจะนำโปรแกรมมาเชื่อมกับโอเอสชั้นในทำได้ยากขึ้น รูปแบบของการทำงานจึงเน้นการแยกโปรเซสและการทำงานระหว่างโปรเซส ออก โดยลดขอบเขตของการทำงานในแต่ละฟังก์ชันลง เพื่อให้สิทธิของแต่ละฟังก์ชันอยู่ระดับต่ำไม่เท่าเทียมกับ root

การเรียกข้อมูลจากระบบ ก็ไม่สามารถเรียกข้อมูลได้โดยตรงแต่จะต้องย้ายส่วนของโอเอสที่เรียกว่าพรอกซี่ เพื่อให้ระบบมีบัฟ-เฟอร์ ผู้ใช้งานจึงเชื่อมสัมผัสกับข้อมูลโฆษณาไม่ได้ ระบบการทำงานแบบ TOS-Trusted OS ได้รับการพัฒนา และเริ่มมีทดลองใช้เพื่อตรวจสอบระบบโดย บริษัท ฮิวเลต แพกการ์ด

การเข้าถึงระบบจากภายนอกจึง เข้าผ่านทาง TOS และเรียกตามฟังก์ชันของการใช้งานเท่านั้น

บริษัทชั้นนำ เช่น IBM ซัน และ HP ได้เน้นการสร้างโอเอสในระบบ TOS กันแล้ว และแนวโน้มจะได้รับการนำมาใช้ในระบบธุรกิจบนเครือข่ายซึ่งต้องอาศัยระบบข้อมูลข่าวสารที่บริการและดูแลบริหารจัดการได้อย่างน่าเชื่อถือ

พัฒนาการของระบบป้องกันยังต้องดำเนินการต่อ

หากจินตนาการดูการแข่งขันระหว่างฝ่ายแฮกเกอร์และฝ่ายพัฒนาระบบจะเห็นว่าทั้งสองฝ่ายมีพัฒนาการไล่กันตลอดเวลา แฮกเกอร์จะหาจุดอ่อนและเรียนรู้ระบบใหม่ ๆ พร้อมทั้งพัฒนาเครื่องมือต่าง ๆ ออกมาใช้ ขณะเดียวกันระบบป้องกันก็พัฒนาวิธีการและรูปแบบการป้องกันแต่ไม่ว่าจะพัฒนาระบบป้องกันอย่างไร การบุกเข้าโจมตี และดำเนินการทางอาชญากรรมคอมพิวเตอร์ก็ยังมีให้เห็นเหมือนกับระบบสังคมในปัจจุบันที่ยังมีโจรผู้ร้ายอยู่ทั้ง ๆ ที่มีระบบยามรักษาความปลอดภัยและกฎหมายที่ดีแล้ว

เอกสารอ้างอิง

1. Sandra Key Miller "The Trusted OS Makes a Comeback" Computer Magazine Vol 34, No. 2 Feb 2001 pp. 16-19